Michael Connett (SBN 283360)
**SIRI & GLIMSTAD LLP**
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: (772) 783-8436
mconnett@sirillp.com

Tyler J. Bean*
Sonjay C. Singh*
**SIRI & GLIMSTAD LLP**
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (772) 783-8436
tbean@sirillp.com
ssingh@sirillp.com

**UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF CALIFORNIA**

| | |
|---|---|
| **M.S.** AND **C.P.**, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED<br>Plaintiff,<br><br>vs.<br><br>**AYLO GLOBAL ENTERTAINMENT, INC.** AND **AYLO USA INCORPORATED**,<br><br>Defendants. | **Civil Action No.: 2:25-cv-01139-DJC-JDP**<br><br>**AMENDED CLASS ACTION COMPLAINT** |

Plaintiffs M.S. and C.P. (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendants Aylo Global Entertainment, Inc. and Aylo USA Incorporated (collectively, "Defendants" or "Pornhub") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

## I. INTRODUCTION

1. A person's sexual desires are some of the most sensitive, personal things in life. As the Supreme Court has stated, an individual's sexual behavior within their own home represents the "most private human conduct…in the most private of places." *Lawrence v. Texas*, 539 U.S. 558, 567 (2003).

2. For a majority of Americans, their sexual lives in some way involve viewing pornography. Even though the statistics vary, a 2020 academic study reported that "[u]sing all modalities of pornography, 91.5% of men and 60.2% of women herein reported having consumed pornography in the past month."[1] Likewise, according to a 2023 research article reported on in Psychology Today:

> Using a set of metrics that includes indicators of monthly unique visitors as well as monthly pageviews, the authors [of the article in the Journal Of Sex Research] found that the top three pornography sites are more highly ranked than the most well-known household name sites (Amazon, Netflix, Yahoo) as well as those that are the most up and coming (TikTok, OpenAI/ChatGPT, Zoom).[2]

[1] Solano, Eaton & O'Leary, *Pornography Consumption, Modality and Function in a Large Internet Sample* (J. Sex Res. Jan. 2020) *available at* https://pubmed.ncbi.nlm.nih.gov/30358432/

[2] McNichols, Nicole K. Ph.D., *How Many People Actually Watch Porn*? (Psychology Today Sept. 25, 2023) *available at* https://www.psychologytoday.com/us/blog/everyone-on-top/202309/how-much-porn-do-americans-really-watch (reporting on Wright, Tokunaga & Herbenick, *But*

That result is consistent with a similar study performed a decade earlier, which found that pornography sites were unquestionably the most popular on the internet.

3. Yet despite its prevalence, pornography usage is still something people do not discuss. For example, a large percentage of couples in a 2021 study reported that their significant other does not know the frequency of pornography that they watch.[3] It is not surprising that people want to keep their pornography usage to themselves, as many people still disapprove of it and the effects it can have on participants and relationships.[4] Thus, it is clear that pornography usage is an extremely private thing that while most people do it, they do not want anyone to know about it.

4. Pornhub is one of the most popular pornography destinations on the internet. It hosts a wide range of pornographic content including millions of pornographic videos.[5] It alone is the nineteenth most-visited

---

*Do Porn Sites Get More Traffic than TikTok, OpenAI, and Zoom?,* 763-767 (J. Sex Res. June 5, 2023) *available at* https://www.tandfonline.com/doi/full/10.1080/00224499.2023.2220690)

[3] Crawford & Butler, *The Truth Hurts Less: Pornography Use Disclosure vs. Deception* (Inst. for Family Stud. July 7, 2021) *available at* https://ifstudies.org/blog/the-truth-hurts-less-pornography-use-disclosure-vs-deception ("In a nationally representative study of couples in committed relationships, 37% of men reported more pornography use than their partner believed was occurring. In casually dating relationships, 43% of the men reported using pornography daily or every other day, while none of their partners reported awareness of that level of use.")

[4] Carroll & Willoughby, *The Porn Gap: Gender Differences in Pornography Use in Couple Relationships* (Inst. for Family Stud. Oct. 5, 2017) *available at* https://ifstudies.org/blog/the-porn-gap-gender-differences-in-pornography-use-in-couple-relationships.

[5] Zoe Haylock, *Pornhub Just Deleted Most of Its Content*, VULTURE (Dec. 14, 2020), https://www.vulture.com/2020/12/pornhub-deletes-all-unverified-content-millions-of-videos.html (last visited Apr. 16, 2025).

website on the entire Internet, with its Website —www.pornhub.com (the "Website")— receiving *billions* of visits each year.[6]

5. Plaintiffs used Defendants' Website to privately view pornographic media from the comfort of their own homes. Given how confidential the entire subject is, when Plaintiffs used the Website, they assumed that Pornhub would do its utmost to keep their use of its service private.

6. Unfortunately, unbeknownst to Plaintiffs and other visitors to the Website, Pornhub does not keep sensitive information about their Website visitors private. Instead, Defendants collect and transmit information related to individuals' use of the Website, including the specific pornographic videos that they watch (the "Sensitive Information"), to third party advertisers, including Alphabet Inc. ("Google"), through the use of surreptitious online tracking tools.

7. Online advertising giants, like Google, try to compile as much information as possible about American consumers, including the most private aspects of their lives, as fuel for a massive, targeted advertising enterprise. Any information about a person captured by those online behemoths can be used to stream ads to that person. If Google receives information that a person views pornography, it will use that information, and allow its clients to use that information, to stream ads to that person's computers and smartphones relating to the specific types of pornography that the person consumes.

[6] *Top Websites*, SIMILARWEB (Feb. 2025), https://www.similarweb.com/top-websites/ (last visited Apr. 16, 2025).

8. Google offers website operators access to its proprietary suites of marketing, advertising, and customer analytics software, including Google Analytics, Google AdSense, and Google Tag Manager (collectively, the "Business Tools"). Armed with these Business Tools, website operators can leverage Google's enormous database of consumer information for the purposes of deploying targeted advertisements, performing minute analyses of their customer bases, and identifying new market segments that may be exploited.

9. But, in exchange for access to these Business Tools, website operators install Google's surveillance software on their website (the "Tracking Tools"), including 'tracking pixels' ("Pixels") and third-party 'cookies' that capture sensitive, personally identifiable information provided to the website operator by its website users. This sensitive information can include a unique identifier that Google uses to identify that user, regardless of what computer or phone is used to access the website. The Tracking Tools can also capture and share other information like the specific webpages visited by a website user, items added to an online shopping cart by a website user, information entered into an online form by a website user, and the device characteristics of a website user's phone or computer.

10. In essence, when website operators use Google's Business Tools, they choose to participate in Google's mass surveillance network and, in turn, benefit from Google's collection of user data at the expense of their customers' privacy.

11. Pornhub chose to accept the devil's bargain offered by Google by installing Google's Tracking Tools on the Website. In doing so, they have chosen to prioritize marketing over customer privacy.

12. Each of the Plaintiffs and Class Members visited the Website and had their personal Sensitive Information tracked by Defendants using the Tracking Tools. However, Defendants ***never*** obtained informed consent from Plaintiffs or Class Members to share the Sensitive Information it collects with third parties, let alone with Google, the largest advertiser and compiler of user information in the world.

13. Moreover, Defendants' tracking of Website users violated numerous state and federal laws, including the Video Privacy Protection Act ("VPPA"), passed specifically to prevent the disclosure and aggregation of data relating to an individual's video consumption.

14. As a result of Defendants' conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with online service providers; (iii) emotional distress and heightened concerns related to the release of Sensitive Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of the Sensitive Information; (vi) statutory damages and (viii) continued and ongoing risk to their Sensitive Information.

15. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: Invasion of Privacy; Breach of Confidence; Negligence; Breach of Implied Contract; violations of the Video Privacy Protection Act ("VPPA"), 18

U.S.C. § 2710, *et seq.*; violations of the Electronic Communications Privacy Act ("ECPA"); violations of N.Y. Gen. Bus. Law § 349; violations of the California Invasion of Privacy Act ("CIPA"); Cal. Pen. Code § 360, *et seq.*; and violations of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code, § 17200, *et seq*.

## II. PARTIES

***Plaintiff M.S.***

16. Plaintiff M.S. is a citizen of the state of California, residing in El Dorado County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

17. Plaintiff M.S. registered for an account on the Website and utilized it on his personal electronic devices on multiple occasions in 2024 and 2025, to view pornographic media, including paid content.

18. Unbeknownst to Plaintiff M.S., the Tracking Tools contemporaneously transmitted the Sensitive Information that was communicated to and from Plaintiff M.S. as he used the Website, including the specific videos that he viewed.

19. Plaintiff M.S. never authorized Defendants to disclose any aspect of his communications with Defendants through the Website to third parties.

20. On every occasion that he visited Defendants' Website, Plaintiff M.S. possessed an account with Google, and he accessed Defendants' Website while logged into his Google account on the same device.

***Plaintiff C.P.***

21. Plaintiff C.P. is a citizen of the state of New York, residing in Richmond County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

22. Plaintiff C.P. registered for an account on the Website and utilized it on his personal electronic devices on multiple occasions in 2024 and 2025, to view pornographic media.

23. Unbeknownst to Plaintiff C.P., the Tracking Tools contemporaneously transmitted the Sensitive Information that was communicated to and from Plaintiff C.P. as he used the Website, including the specific videos that he viewed.

24. Plaintiff C.P. never authorized Defendants to disclose any aspect of his communications with Defendants through the Website to third parties.

25. On every occasion that he visited Defendants' Website, Plaintiff C.P. possessed an account with Google, and he accessed Defendants' Website while logged into his Google account on the same device.

***Defendant Aylo Global Entertainment, Inc.***

26. Defendant Aylo Global Entertainment, Inc. is a limited liability corporation incorporated in Delaware with its principal place of business at 610 Brazos St, Suite 500 Austin, Texas 78701. Defendant Aylo Global Entertainment, Inc. operates the Website.

***Defendant Aylo Usa Incorporated***

27. Defendant Aylo USA Incorporated is a limited liability corporation incorporated in Delaware with its principal place of business

at 610 Brazos St, Suite 500 Austin, Texas 78701. Defendant Aylo USA Incorporated operates the Website.

## III. JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

29. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*) and VPPA (18 U.S.C. § 2710, *et seq.*).

30. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein from part of the same case or controversy.

31. This Court has personal jurisdiction over Defendants because Defendants have advertised and offered their Website to consumers in the State of California and in this judicial district. Personal jurisdiction is also proper because Defendants committed tortious acts in the State of California and this judicial district and Plaintiffs' claims arise out of such acts, and/or because Defendants have otherwise made or established contacts in the State of California and in this judicial district sufficient to permit the exercise of personal jurisdiction.

32. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims in this action occurred in this judicial district.

## IV. FACTUAL ALLEGATIONS

### A. THE VIDEO PRIVACY PROTECTION ACT

33. The VPPA was passed in 1988 in response to Congress's concern that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

34. In passing the VPPA, Congress was particularly alarmed about surveillance of Americans' media consumption, recognizing that:

> Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy-of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye…These records are a window into our loves, lives, and dislikes.

*Id*. (statement of Rep. Al McCandless).

35. Although the VPPA was originally intended to protect the privacy of an individual's rental videotape selections, Congress has repeatedly reiterated that the VPPA is applicable to "'on-demand' cable services and Internet streaming services [that] allow consumers to watch

movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at p. 2.[7]

36. Under the VPPA, "[a] video tape service provider" is prohibited from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider" without the consumer's "informed, written consent… in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer." 18 U.S.C. § 2710(b).

37. The VPPA defines a "video tape service provider" as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio-visual materials." 18 U.S.C. § 2710(a)(4).

38. The VPPA additionally defines "personally identifiable information" as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3).

39. Defendants are inarguably video tape services provider under the meaning of the VPPA, as its primary business is monetizing access to the millions of pornographic videos hosted on the Website. Accordingly, Defendants' disclosure of the specific videos viewed by

[7] *See also The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW (Jan. 31, 2012), *available online at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-videoprivacy-protection-act-protecting-viewer-privacy-in-the-21st-century (statement by Senator Leahy, who originally introduced the VPPA in the Senate: "Now, it is true that technology has changed…but I think we should all agree that we have to be faithful to our fundamental right to privacy and freedom. Today the social networking, video streaming, the cloud, mobile apps, and other new technologies have revolutionized the availability of Americans' information.").

users of the Website, like Plaintiffs', constitutes a violation of VPPA. *See*, *e.g.*, *Fan v. NBA Props. Inc.*, No. 23-cv-05069-SI, 2024 U.S. Dist. LEXIS 57205, at *9 (N.D. Cal. Mar. 26, 2024) ("in enacting the VPPA, 'Congress[] inten[ded] to cover new technologies for pre-recorded video content'" and "used 'similar audio visual materials' to ensure that VPPA's protections would retain their force even as technologies evolve").

## B. DEFENDANTS' USE OF THIRD-PARTY TRACKING TECHNOLOGIES

### a. Google's Mass Advertising Surveillance Operation

40. Google is the largest digital advertiser in the country, accounting for 26.8-percent of the total digital advertising revenue generated in the United States.[8] In 2023, Google's advertising revenue of $238 billion accounted for 77-percent of its total revenue for the year.[9]

41. Google advertises Google Analytics and other Business Tools to website operators, like Defendants, claiming they will allow the operator to "[u]nderstand [their] site and app users," "check the performance of [their] marketing," and "[g]et insights only Google can

[8] *Share of major ad-selling companies in digital advertising revenue in the United States*, STATISTA (May 2024), https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last visited Feb. 1, 2025).

[9] Florian Zandt, *Google's Ad Revenue Dwarfs Competitors*, STATISTA (Sep. 10, 2024), https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year (last visited Feb. 1, 2025).

give."[10] But, in order for website operators to get information from Google Analytics about their website's visitors, they must allow data collection through installation of Google's Tracking Tools on their website.[11]

42. Indeed, on its *Privacy & Terms* page, Google admits that it collects information from third party websites, stating that: "[m]any websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google."[12]

43. Google also admits that it uses the information collected from third party websites, such as Defendants', to sell targeted advertising, explaining to users that: "[f]or example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google."[13]

44. Even though Google admits that it collects information from third-party websites through the Tracking Tools, it does not provide, nor could it provide, a publicly available list of every webpage on which its Tracking Tools are installed. As such, the vague descriptions of Google's

---

[10] *Welcome to Google Analytics*, GOOGLE, https://analytics.google.com/analytics/web/provision/?authuser=0#/provision (last visited Feb. 1, 2025).

[11] *See* Aaron Ankin & Surya Matta, *The High Privacy Cost of a "Free" Website*, THE MARKUP, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites (last visited Feb. 1, 2025).

[12] *Privacy & Terms – How Google uses information from sites or apps that use our services*, GOOGLE, https://policies.google.com/technologies/partner-sites (last visited Feb. 1, 2025).

[13] *Id.*

data collection practices referenced above could not give Plaintiffs and Class Members any reason to think that Defendants were part of Google's surveillance network.

45. Google aggregates the user information that it collects from third-party websites into 'advertising profiles' consisting of all of the data that it has collected about a given user.[14] With these advertising profiles, Google can sell hyper-precise advertising services, allowing its clients to target internet users based on combinations of their location, age, race, interests, hobbies, life events (*e.g.*, recent marriages, graduation, or relocation), political affiliation, education level, home ownership status, marital status, household income, type of employment, use of specific apps or websites, and more.[15]

46. Google's surveillance of individual's internet usage is ubiquitous. In 2017, Scientific American reported that over 70-percent of smartphone apps report "personal data to third-party tracking companies like Google,"[16] and Google trackers are present on 74-percent of all web traffic.

[14] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), *available online at*: https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

[15] *About audience segments*, GOOGLE ADS, https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics (last visited Feb. 1, 2025).

[16] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCIENTIFIC AMERICAN (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last visited Feb. 1, 2025).

47. Moreover, as in this case, the data collected by Google often pertains to the most personal and sensitive aspects of an individual's life. For example:

a. 81-percent of the most popular mobile apps for managing depression and quitting smoking allowed Facebook and/or Google to access subscriber information, including health diary entries and self-reports about substance abuse.[17]

b. Twelve of the largest pharmacy providers in the United States send information regarding user's purchases of products such as pregnancy tests, HIV tests, prenatal vitamins, and Plan B to online advertisers.[18] For example, when an online shopper searches for a pregnancy test, views the product page for a pregnancy test, or adds a pregnancy test to their online shopping cart on Kroger's website, that information is transmitted to Google.[19]

48. This monumental, invasive surveillance of Americans' internet usage is not accidental. As Google's then-CEO Eric Schmit

[17] Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN (2019), *available online at*: https://pubmed.ncbi.nlm.nih.gov/31002321/.

[18] Darius Tahir & Simon Fondrie-Teitler, *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*, THE MARKUP (June 30, 2023), https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it (last visited Feb. 1, 2025).

[19] Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, THE MARKUP (Feb. 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you (last visited Feb. 1, 2025).

admitted in 2010: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[20]

49. In fact, Google values user information so highly that it provides its Business Tools to many website operators for free, all to expand its surveillance apparatus.[21]

50. When website operators, like Defendants, make use of Google's Business Tools, they are essentially choosing to participate in Google's mass surveillance network, and in return they benefit from Google's collection of user data, at the expense of their website users' privacy. For example, Google rewards website operators for providing it with their user's information by granting access to its Analytics platform, which leverages demographic data collected by Google to provide detailed analyses of the website's user base.[22]

**b. Pixels Can Record Almost Every Interaction Between a User and a Website**

51. In order to use Google's Business Tools, Defendants installed Google's Tracking Tools, including tracking Pixels, onto the Website.

[20] Andrew Orlowski, *Google's Schmidt: We know what you're thinking*, THE REGISTER (Oct. 4, 2020), https://www.theregister.com/2010/10/04/google_ericisms/ (last visited Feb. 1, 2025).

[21] *Analytics Overview*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Feb. 1, 2025) ("Google Analytics gives you the tools, free of charge"),

[22] *Google Marketing Platform – Features*, GOOGLE, https://marketingplatform.google.com/about/analytics/features/ (last visited Feb. 1, 2025).

52. Pixels are one of the tools used by website operators to track user behavior. As the Federal Trade Commission ("FTC") explains, a Pixel is:

> [A] small piece of code that will be placed into the website or ad and define [the Pixel operator's] tracking goals such as purchases, clicks, or pageviews…
>
> Pixel tracking can be monetized several ways. One way to monetize pixel tracking is for companies to use the tracking data collected to improve the company's own marketing campaigns…Another is that companies can monetize the data collected by further optimizing their own ad targeting systems and charging other companies to use its advertising offerings.[23]

53. Pixels can collect a shocking amount of information regarding an internet user's online behavior, including the webpages viewed by the user, the amount of time spent by the user on specific webpages, the buttons and hyperlinks that the user clicks while using a website, the items that the user adds to an online shopping cart, the purchases that a user makes through an online retailer, the text entered by the user into a website search bar, and even the information provided by

[23] *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION – OFFICE OF TECHNOLOGY (Mar. 6, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking (last visited Feb. 1, 2025).

the user on an online form.[24]

54. But most internet users are completely unaware that substantial information about their internet usage is being collected through tracking Pixels. The FTC warns that:

> Traditional controls such as blocking third party cookies may not entirely prevent pixels from collecting and sharing information. Additionally, many consumers may not realize that tracking pixels exist because they're invisibly embedded within web pages that users might interact with…Academic and public reporting teams have found that thousands of the most visited webpages have pixels and other methods that leak personal information to third parties.[25]

**c. The Pixels Installed on Defendants' Website Transmit Personally Identifiable Information to Google**

55. Every website is hosted by a computer "server" that holds the website's contents.

56. To access a website, individuals use "web browsers." Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as computer, tablet, or smartphone) accesses web content through a web browser (such as

[24] *See id.*; *How does retargeting on Facebook help your business?*, META, https://www.facebook.com/business/goals/retargeting (last visited Feb. 1, 2025); Tom Kemp, *"Oops! I Did It Again" … Meta Pixel Still Hoovering Up Our Sensitive Data*, MEDIUM, https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last visited Feb. 1, 2025).

[25] *Lurking Beneath the Surface, supra* note 23.

Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge).

57. Communications between a website server and web browser consist of "Requests" and "Responses." Any given browsing session may consist of hundreds or even thousands of individual Requests and Responses. A web browser's Request essentially asks the website to provide certain information, such as the contents of a given webpage when the user clicks a link, and the Response from the website sends back the requested information – the web pages' images, words, buttons, and other features that the browser shows on the user's screen as they navigate the website.

58. Additionally, on most websites, the Response sent back to the user's web browser directs the browser to create small files known as 'cookies' on the user's device.[26] These cookies are saved by the user's web browser, and are used to identify the website user as they browse the website or on subsequent visits to the site.[27] For example, in a more innocuous use case, a cookie may allow the website to remember a user's name and password, language settings, or shopping cart contents.[28]

59. When a Google user logs onto their account, their web browser records a Google tracking cookie.[29] This cookie includes a

[26] *What is a web browser?*, MOZILLA, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (last visited Feb. 1, 2025).

[27] *Id.*

[28] *Id.*

[29] Cyphers, *supra* note 14.

specific line of code that links the web browser to the user's Google account.[30]

60. Google's Pixels use cookies but operate differently than cookies. Rather than directing the browser to save a file on the user's device, the Pixels acquire information from the browser, without notifying the user. The information can include details about the user, his or her interactions with the Website, and information about the user's environment (*e.g.,* type of device, type of browser, and sometimes even the physical location of the device).

61. Simultaneously, the Google Pixels, like those installed on Defendants' Website, request identifying information from any Google cookies previously installed on the user's web browser.

62. The Pixel then combines the data it received from the browser with the data it acquired from the cookie and instructs the web browser to transmit the information back to Google. As a result, Google can link all of the user information collected by their Pixels on the Defendants' Website to the user's identity, via the user's Google profile. Thus, even if a user never actually logs into a website or fills out a form, the website, along with Google, can know the user's identity. This is a particularly troubling thought for many people who view pornography from what they think is the privacy of their own home.

63. A remarkable number of Americans possess a Google account. Just one of Google's many products, its Gmail e-mail client, is

[30] *Id.*

used by over one-third of all Americans.[31] When these internet users visit a website, like Defendants', that utilizes a Google Pixel, any information collected by the Pixel can be linked to the user's identity through the Google cookies installed on the user's web browser.

64. However, it is not only Google account holders that are at risk of having Pixel-collected website data linked to their identities. Rather, Google utilizes sophisticated data tracking methods to identify even those few users who do not have a Google account.

65. Google's Pixels, like those on Defendants' website, can acquire information about the user's device and browser, such as their screen resolution, time zone setting, browser software type and version, operating system type and version, language setting, and IP address.

66. An internet user's combination of such device and browser characteristics, commonly referred to as their "browser fingerprint," is "often unique."[32] By tracking this browser fingerprint, Google is able to compile a user's activity across the internet.[33] And, as Google continuously compiles user data over time, its understanding of the user's browser fingerprint becomes more sophisticated such that it needs only to collect a single piece of identifying information to identify the user linked to a browser fingerprint.

---

[31] *See* Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024), https://techjury.net/blog/gmail-statistics/ (last visited Feb. 1, 2025) ("Gmail accounts for 130.9 million of the total email users in the US"). The United States population is approximately 337.4 million. *See* UNITED STATES CENSUS BUREAU, https://www.census.gov/popclock/ (last visited Feb. 1, 2025).

[32] Cyphers, *supra* note 14.

[33] *Id*.

**d. Defendants Disclosed Plaintiffs' and Class Members' Sensitive Information to Google**

67. Unbeknownst to Plaintiffs and Class Members, Defendants intentionally configured the Google Pixels installed on the Website to capture and transmit an enormous amount of the Sensitive Information about them and their use of the Website.

68. In their default state as provided by Google, Google's Pixels record and transmit only "automatic events," consisting largely of routine user behavior, such as clicking a link, clicking on an advertisement, or viewing a webpage. However, the Google Pixels used on Defendants' Website are not in their default state. Instead, Defendants intentionally configured the Pixels on the Website to collect and transmit large amounts of additional user data.

69. The below screenshot ("Figure 1") shows the information requested and transmitted to Google by the Pixels installed on Defendants' Website. The information provided in Figure 1 is exemplar information collected on Defendants' Website, and is not Plaintiffs' information, but the Pixels installed on Defendants' Website collected the same or similar information about Plaintiffs. This includes not just the fact that the user is watching a Pornhub video and the URL of the video, but also the title of the video (in this example it appears next to the cookie labeled "dt:"), the language spoken in the video (next to the cookie labeled "ep.language_spoken_in_video"), the date that the video was uploaded onto Pornhub (next to the cookie labeled "ep.video_date_published"), the sexual orientation associated with the video (e.g., straight, gay, here next to the cookie labeled "ep.video_segment"), whether the video contained

formal "pornstars" (next to the cookie labeled "ep.pornstars_in_video"), and the production company that uploaded the video (next to the cookie labeled "ep.video_uploaded_name").

70. All of this information that Defendant transmitted to Google was accompanied by specific lines of code linking the Sensitive Information provided by Plaintiffs and Class Members to their identities. The following screenshot shows that the Google Pixel on Defendants' Website transmitted the identifier number attached to Google's "cid" cookie, which identify the user's Google account, along with other information that is commonly used to create a browser fingerprint, such as the user's language preference, screen resolution, browser software and version, operating system software and version, device type (e.g. PC, mobile phone), network type (e.g., cellular, LAN), and internet service provider.


Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Query String Parameters
view source
view URL-encoded
v: 2
tid: G-B39RFFWGYY
gtm: 45je54f1v889308053z8892446692za200zb892446692
_p: 1744843151978
gcs: G111
gcd: 13t3t3l3l5l1
npa: 0
dma: 0
tag_exp: 102509683~102803279~102813109~102887800~102926062~103027016~103051953~103055465~103077950~10
3106314~103106316
cid: 87303652.1744773621
ul: en-us
sr: 1920x1080
uaa: x86
uab: 64
uafvl: Google%20Chrome;135.0.7049.85|Not-A.Brand;8.0.0.0|Chromium;135.0.7049.85
uamb: 0
uam:
uap: Windows
uapv: 19.0.0
uaw: 0
are: 1
pae: 1
frm: 0
pscdl: noapi
_eu: AAAAAAI
_s: 1
sid: 1744843099
sct: 4
seg: 1
dl: https://www.pornhub.com/view_video.php?viewkey=67e9cef024d29
dr: https://www.pornhub.com/video
dt: Fuck me while no one's looking - Pornhub.com
en: page_view
ep.active: active
ep.hd_video: Yes


*Figure 1. Screenshot depicting back-end network traffic from the Website which shows information transmitted to Google when Website users watch a video.*

71. By installing third-party Tracking Tools, including tracking Pixels, on the Website, and by further custom configuring those Pixels to collect their Website users' Sensitive Information, Defendants knowingly

and intentionally caused Plaintiffs' and Class Members' Sensitive Information to be transmitted to third parties, including Google.

### C. DEFENDANTS DISCLOSED PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES WITHOUT THEIR KNOWLEDGE OR CONSENT

#### a. The Tracking Tools Used by Defendants Were Imperceptible to Plaintiffs and Class Members

72. The Tracking Tools installed on Defendants' Website were invisible to Plaintiffs and Class Members. Without analyzing the network information transmitted by Defendants' Website through examination of its source code or the use of sophisticated web developer tools, there was no way for a Website user to discover the presence of the Tracking Tools. As a result, typical internet users, such as Plaintiffs and Class Members, were unable to detect the Tracking Tools on Defendants' Website.

73. Plaintiffs and Class Members were shown no disclaimer or warning that their Sensitive Information would be disclosed to any unauthorized third party without their express consent.

74. Plaintiffs and Class Members did not know that their Sensitive Information was being collected and transmitted to an unauthorized third party.

75. Because Plaintiffs and Class Members were not aware of the Google Pixels on Defendants' website, or that their Sensitive Information would be collected and transmitted to Google, they could not and did not consent to Defendants' conduct.

## D. DEFENDANTS WERE ENRICHED BY ITS DISCLOSURE OF PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES

### a. Defendants Received Material Benefits in Exchange for Plaintiffs' Sensitive Information

76. As explained, *supra*, users of Google's Business Tools, like Defendants, receive access to advertising and marketing analytics services in exchange for installing Google's Tracking Tools on their website.

77. Upon information and belief, Defendants, as users of Google's Business Tools, received compensation in the form of advanced advertising services and cost-effective marketing on third-party platforms in exchange for allowing Google to collect Plaintiffs' and Class Members' Sensitive Information.

### b. Plaintiffs' and Class Members' Data Had Financial Value

78. Moreover, Plaintiffs' and Class Members' Sensitive Information had value, and Defendants' disclosure and interception of that Sensitive Information harmed Plaintiffs and the Class.

79. According to the financial statements of Facebook, another major seller of online advertisements, the value derived from user data has continuously risen. "In 2013, the average American's data was worth about $19 per year in advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth $164 per year."[34]

[34] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/ (last visited Feb. 1, 2025).

80. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

81. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

82. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Information has diminished the value of that information, resulting in harm including Plaintiffs and Class Members.

**E. PLAINTIFFS' AND CLASS MEMBERS' REASONABLE EXPECTATION OF PRIVACY**

83. At all times when Plaintiffs and Class Members provided their Sensitive Information to Defendants, they each had a reasonable expectation that the information would remain confidential and that Defendants would not share the Sensitive Information with third parties for a commercial purpose, unrelated to processing their loan applications.

84. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative informed consent before a company collects and shares that individual's data to be one of the most important privacy rights.

85. For example, a recent Consumer Reports study shows that 92-percent of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer

data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[35]

86. Individuals are particularly sensitive about disclosure of information relating to pornography usage. Extensive research has shown that pornography usage is nearly ubiquitously linked to significant feelings of shame, particularly because of the societal stigma attached to the consumption of pornography.[36] As a result, qualitative studies have showed that the most common behavior among those who consume pornography is "keeping their pornography viewing secret from others, such as partners and family."[37]

[35] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907 (last visited Feb. 1, 2025).

[36] *See* Wendy G. Macdowall, *et al*., *Pornography Use Among Adults in Britain: A Qualitative Study of Patterns of Use, Motivations, and Stigma Management Strategies*, ARCH. SEX. BEHAV. (Apr. 3, 2025), at p. 2, *available online at*: https://link.springer.com/article/10.1007/s10508-025-03112-7 (compiling studies finding shame and social stigma associated with pornography); Luke Sniewski and Pani Farvid, *Hidden in Shame: Heterosexual Men's Experiences of Self-Perceived Problematic Pornography Use*, 21(2) PSYCH. MEN & MASC. 210 (July 18, 2019), *available online at*: https://www.lukesniewski.com/wp-content/uploads/2019/09/Hidden-in-Shame.pdf ("The main reason men kept their viewing hidden from the world was because of the accompanying experiences of guilt and shame that would inevitably follow most—if not all—viewing sessions"); Michael Tholander, Sofia Johansso, Klara Thunell and Örjan Dahlström, *Traces of Pornography: Shame, Scripted Action, and Agency in Narratives of Young Swedish Women*, 26 SEXUAL. & CULT. 1826 (May 11, 2022) (noting "private and silent shame" associated with pornography consumption due to attitudes that viewing pornography is "'dirty,' 'disgusting,' 'hideous,' 'repugnant," 'unnatural,' and 'vulgar'"), *available online at*: https://link.springer.com/article/10.1007/s12119-022-09973-7/.

[37] Macdowall, *supra* note 32, at pp. 3-8.

87. Personal data privacy and obtaining consent to share Sensitive Information are material to Plaintiffs and Class Members.

## V. TOLLING AND ESTOPPEL

88. Any applicable statutes of limitation have been tolled by Defendants' knowing and active concealment of its incorporation of Google's Tracking Tools into the Website.

89. The Pixels and other tracking tools on Defendants' Website were and are invisible to the average website visitor.

90. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendants' deception and unlawful conduct.

91. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

92. Defendants had exclusive knowledge that the Website incorporated the Pixels and other Tracking Tools and yet failed to disclose to customers, including Plaintiffs and Class Members, that by visiting the Website, Plaintiffs' and Class Members' Sensitive Information would be disclosed or released to unauthorized third parties, including Google.

93. Under the circumstances, Defendants were under a duty to disclose the nature, significance, and consequences of their collection and treatment of Website users' Sensitive Information. In fact, Defendants still have not conceded, acknowledged, or otherwise indicated to their customers that they have disclosed or released their Sensitive Information to unauthorized third parties. Accordingly, Defendants are estopped from relying on any statute of limitations.

94. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

95. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendants' conduct would have been shortly before the filing of this Complaint.

## VI. CLASS ALLEGATIONS

96. This action is brought by the named Plaintiffs both individually, and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

97. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

**The Nationwide Class**

All natural persons who watched a video on the Website, and whose Sensitive Information was disclosed or transmitted to Google or any other unauthorized third party.

98. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of separate California and New York Subclasses, which are defined as follows:

**California Subclass**

All natural persons residing in California who watched a video on the Website, and whose Sensitive Information was disclosed or transmitted to Google or any other unauthorized third party.

**New York Subclass**

All natural persons residing in New York who watched a video on

the Website, and whose Sensitive Information was disclosed or transmitted to Google or any other unauthorized third party.

99. Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; and any Judge conducting any proceeding in this action and members of their immediate families.

100. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

101. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 10,000 individuals that have been impacted by Defendants' actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendants.

102. **Commonality.** Common questions of law or fact arising from Defendants' conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

a) Whether and to what extent Defendants had a duty to protect the Sensitive Information of Plaintiffs and Class Members;

b) Whether Defendants had duties not to disclose the Sensitive Information of Plaintiffs and Class Members to unauthorized third parties;

c) Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

d) Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Sensitive Information was being disclosed without their consent;

e) Whether Defendants adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' Sensitive Information;

f) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to keep the Sensitive Information belonging to Plaintiffs and Class Members free from unauthorized disclosure;

g) Whether Defendants violated the Video Privacy Protection Act, as alleged in this Complaint;

h) Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

i) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendants' disclosure of their Sensitive Information.

103. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Information, like that of every other Class Member, was compromised as a result of Defendants' incorporation and use of the Tracking Tools.

104. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

105. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including third parties, like Google, in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

106. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy.

The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

107. Defendants acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

108. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information and not disclosing it to unauthorized third parties;

b) Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

c) Whether Defendants failed to comply with applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

e) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendants' wrongful conduct.

109. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the unauthorized disclosures that have taken place.

**COUNT I**

**COMMON LAW INVASION OF PRIVACY - INTRUSION UPON SECLUSION**

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and New York Subclasses)***

110. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 109 as if fully set forth herein.

111. Plaintiffs and Class Members have an interest in: (1)

precluding the dissemination and/or misuse of their sensitive, highly personal Sensitive Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to the exfiltration of their communications without Plaintiffs' and Class Members' knowledge or consent.

112. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via the Website and the communications platforms and services therein.

113. Plaintiffs and Class Members communicated Sensitive Information that they intended for only Defendants to receive and that they understood Defendants would keep private and secure.

114. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and informed consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

115. Plaintiffs and Class Members have a general expectation that their communications regarding sensitive, highly personal information would be protected from surreptitious disclosure to third parties.

116. Defendants' disclosure of Plaintiffs' and Class Members' Sensitive Information coupled with individually identifying information is highly offensive to the reasonable person.

117. As a result of Defendants' actions, Plaintiffs and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

118. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to compensatory and/or nominal damages.

119. Plaintiffs and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

120. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendants' actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

121. Plaintiffs also seek such other relief as the Court may deem just and proper.

## COUNT II

## NEGLIGENCE

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and New York Subclasses)***

122. Plaintiffs repeat and reallege the allegations contained in paragraphs 110 through 121 as if fully set forth herein.

123. Through using Defendants' Website, Plaintiffs and Class Members provided them with their Sensitive Information.

124. By collecting and storing data related to Plaintiffs and Class Members use of the Website, Defendants had a duty of care to use reasonable means to secure and safeguard it from unauthorized disclosure to third parties.

125. Defendants negligently, recklessly, and/or intentionally failed to take reasonable steps to protect Plaintiffs' and Class Members' Sensitive Information from being disclosed to third parties, without their consent, including to Google.

126. Defendants further negligently, recklessly, and/or intentionally omitted to inform Plaintiffs and the Class that they would use their Sensitive Information for marketing purposes, or that their Sensitive Information would be transmitted to third parties.

127. Defendants knew, or reasonably should have known, that Plaintiffs and the Class would not have provided their Sensitive Information to Defendants, had Plaintiffs and the Class known that Defendants intended to use that information for unlawful purposes.

128. Defendants' conduct has caused Plaintiffs and the Class to suffer damages by having their highly confidential, personally identifiable Sensitive Information accessed, stored, and disseminated without their knowledge or consent.

129. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages.

130. Defendants' negligent conduct is ongoing, in that they still hold the Sensitive Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) cease collection and dissemination of the Website users' Sensitive Information to third parties; and (iii) submit to future annual audits of those systems and monitoring procedures.

## COUNT III

## BREACH OF IMPLIED CONTRACT

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and New York Subclasses)***

131. Plaintiffs repeat and reallege the allegations contained in paragraphs 122 through 130 as if fully set forth herein.

132. When Plaintiffs and Class Members provided their Sensitive Information to Defendants in exchange for services, they entered into an implied contract pursuant to which Defendants agreed to safeguard and not disclose their Sensitive Information without consent.

133. Plaintiffs and Class Members accepted Defendants' offers and provided their Sensitive Information to Defendants.

134. Plaintiffs and Class Members would not have entrusted Defendants with their Sensitive Information in the absence of an implied contract between them and Defendants obligating Defendants to not disclose Sensitive Information without consent.

135. Defendants breached these implied contracts by disclosing Plaintiffs' and Class Members' Sensitive Information to third parties like Google.

136. As a direct and proximate result of Defendants' breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

137. Plaintiffs and Class Members would not have used Defendants' services had they known their Sensitive Information would be disclosed.

138. Plaintiffs and Class Members are entitled to compensatory,

consequential, and/or nominal damages as a result of Defendants' breaches of implied contract.

## COUNT IV

## UNJUST ENRICHMENT

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and New York Subclasses)***

139. Plaintiffs repeat and reallege the allegations contained in paragraphs 131 through 138 as if fully set forth herein.

140. Plaintiffs plead this claim in the alternative to their breach of implied contract claim.

141. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for Defendant's services and/or provided their Sensitive Information to Defendants, which Defendants exchanged for marketing and advertising services, as described, *supra*.

142. Defendants knew that Plaintiffs and Class Members conferred these benefits upon them, which Defendants accepted. Defendants profited from Plaintiffs' use of their services, as well as from the Sensitive Information Plaintiffs and Class Members provided by exchanging it for marketing and advertising services.

143. In particular, Defendants enriched themselves by accepting payments made by Plaintiffs and Class Members to view certain content on the Website, and by obtaining the inherent value of Plaintiffs' and Class Members' Sensitive Information and by disclosing such Sensitive Information to third parties, like Google, in exchange for advertising and marketing services.

144. Plaintiffs and Class Members, on the other hand, suffered as

a direct and proximate result of Defendants' decision to prioritize their own profits over the privacy of Plaintiffs' and Class Members' Sensitive Information.

145. Under the principles of equity and good conscience, Defendants should not be permitted to retain these profits obtained by their surreptitious collection and transmission of Plaintiffs' and Class Members' Sensitive Information.

146. If Plaintiffs and Class Members knew that Defendants had not reasonably secured their Sensitive Information, they would not have agreed to provide payment and/or their Sensitive Information to Defendants.

147. Plaintiffs and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damage.

148. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury.

149. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from their surreptitious collection and transmission of Plaintiffs' and Class Members' Sensitive Information, or to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

**COUNT V**

**VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT**

**18 U.S.C. § 2710, *et seq.***

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California Subclass)***

150. Plaintiffs repeat and reallege the allegations contained in paragraphs 139 through 149 as if fully set forth herein.

151. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person[.]" 18 U.S.C. § 2710(b)(1).

152. "Personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

153. A "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

154. Defendants are both a "video tape service provider" because their primary business is the production, hosting, and streaming of millions of videos on the Website, thereby "engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

155. Defendants violated the VPPA by knowingly disclosing Plaintiffs' and Class Members' personally identifiable information to Google through the Tracking Tools without obtaining informed, written consent.

156. As a result of Defendants' violations of the VPPA, Plaintiffs and the Class are entitled to all damages available under the VPPA including declaratory relief, injunctive and equitable relief, statutory damages of $2,500 for each violation of the VPPA, and attorney's fees, filing fees, and costs.

## COUNT VI

## VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), 18 U.S.C. § 2511(1), *et seq*.

### Unauthorized Interception, Use, and Disclosure

***(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and New York Subclasses)***

157. Plaintiffs repeat and reallege the allegations contained in paragraphs 150 through 156 as if fully set forth herein.

158. The ECPA protects both sending and receipt of communications.

159. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

160. The transmissions of Plaintiffs' Sensitive Information to Defendants' Website qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

161. Electronic Communications. The transmission of Sensitive Information between Plaintiffs and Class Members and Defendants' Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

162. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

163. Interception. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

164. Electronic, Mechanical or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendants' web-servers; and

d. The Pixel code deployed by Defendants to effectuate

the sending and acquisition of patient communications.

165. By utilizing and embedding the Pixels on the Website, Defendants intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

166. Specifically, Defendants intercepted Plaintiffs' and Class Members' electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Sensitive Information to third parties such as Google.

167. Defendants' intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Information, including their applications for a debt consolidation loan, and the determination of whether or not to grant those loans.

168. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(c).

169. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

170. Unauthorized Purpose. Defendants intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

171. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

172. Defendants are not parties for purposes to the communication based on their unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendants are parties, Defendants' simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Sensitive Information does not qualify for the party exemption.

173. Defendants' acquisition of sensitive communications that were used and disclosed to Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Invasion of privacy;

b. Breach of confidence;

c. Breach of implied contract;

d. Violations of the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.*;

e. Violations of N.Y. Gen. Bus. Law § 349;

f. Violations of the California Invasion of Privacy Act, Cal.

Pen. Code § 360, *et seq.*; and

g. Violations of the California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq*.

174. Defendants' conduct violated 42 U.S.C. § 1320d-6 in that they used and caused to be used cookie identifiers associated with specific users, including Plaintiffs and Class Members, without user authorization; and disclosed individually identifiable Sensitive Information to Google without user authorization.

175. Defendants are not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that they were participants in Plaintiffs' and Class Members' communications about their Sensitive Information on the Website, because they used their participation in these communications to improperly share Plaintiffs' and Class Members' Sensitive Information with Google and third-parties (a) that did not participate in these communications, (b) that Plaintiffs and Class Members did not know were receiving their Sensitive Information, and (c) that Plaintiffs and Class Members did not consent to receive their Sensitive Information.

176. As such, Defendants cannot viably claim any exception to ECPA liability.

177. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendants' invasion of privacy in that:

a. Learning that Defendants has intruded upon, intercepted, transmitted, shared, and used their Sensitive Information for commercial purposes has caused Plaintiffs and Class Members to suffer

emotional distress;

b. Defendants received substantial financial benefits from their use of Plaintiffs' and Class Members' Sensitive Information without providing any value or benefit to Plaintiffs or Class Members;

c. Defendants received substantial, quantifiable value from their use of Plaintiffs' and Class Members' Sensitive Information, such as understanding how people use the Website and determining what ads people see on the Website, without providing any value or benefit to Plaintiffs or Class Members;

d. The diminution in value of Plaintiffs' and Class Members' Sensitive Information and/or the loss of privacy due to Defendants making such Sensitive Information, which Plaintiffs and Class Members intended to remain private, no longer private.

178. Defendants intentionally used the wire or electronic communications to increase their profit margins. Defendants specifically used the Pixels to track and utilize Plaintiffs' and Class Members' Sensitive Information for financial gain.

179. Defendants were not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

180. Plaintiffs and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading their privacy via the Pixels.

181. Any purported consent that Defendants may claim to have received from Plaintiffs and Class Members was not valid.

182. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendants' Website, Defendants' purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

183. As a result of Defendants' violation of the ECPA, Plaintiffs and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

## COUNT VII

## VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW – DECEPTIVE ACTS OR PRACTICES

### N.Y. Gen. Bus. Law § 349

***(On Behalf of Plaintiff C.P. and the Nationwide Class)***

184. Plaintiffs repeat and reallege the allegations contained in paragraphs 157 through 183 as if fully set forth herein.

185. N.Y. Gen. Bus. Law § 349 prohibits use of "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service[.]"

186. Defendants violated N.Y. Gen. Bus. Law § 349 by:

a. Using the Tracking Technologies to record and transmit the sensitive communications made by and to Plaintiff M.S. and

New York Subclass Members through the Website with third parties, including Google, without their knowledge of consent; and

b. Disclosing the sensitive communications made by and to Plaintiff M.S. and New York Subclass Members through the Website to third parties, including Google, in exchange for marketing and advertising services.

187. Defendants intended to mislead Plaintiff M.S. and New York Subclass Members and intended to induce Plaintiff M.S. and New York Subclass Members to rely on their misrepresentations and omissions.

188. As a result of Defendants' violation of N.Y. Gen. Bus. Law. § 349, Plaintiff M.S. and New York Subclass Members are entitled to actual damages, treble damages, and attorneys' fees, filing fees, and costs.

## COUNT VIII

## VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")

**Cal. Pen. Code § 360, *et seq*.**

***(On Behalf of Plaintiff M.S. and the California Subclass)***

189. Plaintiffs repeat and reallege the allegations contained in paragraphs 184 through 188 as if fully set forth herein.

190. The California Legislature enacted CIPA in response to "advances in science and technology" that "have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications[,]" recognizing that "the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal

liberties and cannot be tolerated in a free and civilized society." Cal. Pen. Code. § 630.

191. Under CIPA, it is unlawful to:

a. "[W]illfully and ***without the consent of all parties to the communication***, or in any unauthorized manner, read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;" or

b. "[U]se, or attempt[] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained[;]" or

c. [A]id, agree[] with, employ[], or conspire[] with any person or persons to unlawfully do, or permit, or cause to be done any of the acts [prohibited by CIPA.]"

Cal. Penal Code § 631(a) (emphasis added).

192. At all relevant times, Defendants aided, employed, agreed with, and conspired with Google, and likely other third parties, to track and intercept Plaintiff M.S.'s and the California Subclass Members' internet communications while using the Website, specifically by installing and configuring the Tracking Tools to permit Google to eavesdrop on and intercept in real-time the content of intercept Plaintiff M.S.'s and the California Subclass Members' private communications with Defendants.

193. The content of those conversations included Sensitive Information, including loan application determinations. Through Defendants' installation and configuration of the Tracking Tools on the Website, these communications were intercepted by Google during the communications and without the knowledge, authorization, or consent of Plaintiff M.S. and the California Subclass Members.

194. Defendants intentionally inserted an electronic device into their Website that, without the knowledge and consent of Plaintiff M.S. and California Subclass Members, transmitted the substance of their confidential communications with Defendants to third parties.

195. Defendants willingly facilitated Google's and other third parties' interception and collection of Plaintiff M.S.'s and California Subclass Members' Sensitive Information by embedding the Tracking Tools on the Website, thereby assisting Google's eavesdropping.

196. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Tracking Tools falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Google and other third parties used to track intercept Plaintiff M.S.'s and the California Subclass Members' communications while they were navigating the Website;

b. Plaintiff M.S.'s and the California Subclass Members' internet browsers;

c. Plaintiff M.S.'s and the California Subclass Members' computing and mobile devices;

d. Google's web and ad servers;

e. The web and ad servers from which Google and other third parties tracked and intercepted Plaintiff M.S.'s and the California Subclass Members' communications while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by Google and other third parties to effectuate their tracking and interception of Plaintiff M.S.'s and the California Subclass Members' communications while they were using a browser to visit the Website; and

197. As demonstrated hereinabove, Defendants violate CIPA by aiding and permitting third parties, including Google and their agents, employees, and contractors to receive Plaintiff M.S.'s and the California Subclass Members' Sensitive Information in real time through the Website without their consent

198. By disclosing Plaintiff M.S.'s and the California Subclass Members' Sensitive information, Defendants violated Plaintiff M.S.'s and California Subclass Members' statutorily protected right to privacy.

199. As a result of Defendants' violation of the CIPA, Plaintiff M.S. and the California Subclass Members are entitled to treble actual damages related to their loss of privacy in an amount to be determined at trial, statutory damages, attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages.

**COUNT IX**

**VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")**

**Cal. Bus. & Prof. Code, § 17200, *et seq.***

***(On Behalf of Plaintiff M.S. and the California Subclass)***

200. Plaintiffs repeat and reallege the allegations contained in paragraphs 189 through 199 as if fully set forth herein.

201. The UCL prohibits any "unlawful, unfair or fraudulent business act or practice" and any "unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code, § 17200.

202. Defendants violated the "unlawful" prong of the UCL by violating Plaintiff M.S.'s and California Subclass Members' right to privacy, as well as by violating the statutory counts alleged herein.

203. Defendants violated the unfair prong of the UCL by:

a. Using the Tracking Technologies to record and transmit the sensitive communications made by and to Plaintiff M.S. and the California Subclass Members through the Website with third parties, including Google, without their knowledge or consent; and

b. Disclosing the sensitive communications made by and to Plaintiff M.S. and the California Subclass Members through the Website to third parties, including Google, in exchange for marketing and advertising services.

204. As a result of Defendants' violations of the UCL, Plaintiff M.S. and the California Subclass Members have suffered the diminution of the value of their Sensitive Information, as alleged above.

205. As a result of Defendants' violation of the UCL, Plaintiff M.S. and the California Subclass Members are entitled to injunctive relief, as well as restitution necessary to restore to them in interest any money or property, real or personal, acquired through Defendants' unfair competition practices.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, individually and on behalf of other Class Members, pray for judgment against Defendants as follows:

A. an Order certifying the Nationwide Class, and California and New York Subclasses, and appointing the Plaintiffs and their Counsel to represent the Classes;

B. equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiffs and Class Members;

C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation

expenses, as allowed by law;

F. prejudgment interest on all amounts awarded; and

G. all such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demand a jury trial on all issues so triable

Dated: June 25, 2025

Respectfully submitted

*/s/ Michael Connett*
Michael Connett
mconnett@sirillp.com
**SIRI & GLIMSTAD LLP**
700 S. Flower Street,
Ste. 1000
Los Angeles, CA
90017
Telephone: (772) 783-8436

Tyler J. Bean*
Sonjay C. Singh*
**SIRI & GLIMSTAD LLP**
745 Fifth Avenue,
Suite 500
New York, New York
10151
Tel: (212) 532-1091
E: tbean@sirillp.com
E: ssingh@sirillp.com

**pro hac vice*

***Attorneys for Plaintiffs and the Class***